




**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

December 18, 2013

TO: Jonathan E. Fielding M.D., M.P.H., Director
Department of Public Health

FROM: Wendy L. Watanabe
Auditor-Controller 

SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW – TORRANCE
PUBLIC HEALTH CENTER**

We have completed a review of the Department of Public Health (DPH) Torrance Public Health Center's (TPHC) compliance with the Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic Clinical Health (HITECH) Act.¹ On November 13, 2013, we provided your Department with our final draft report, and conducted an exit conference on December 16, 2013. This report includes our recommendations and your Department's response(s).

Approach/Scope

The purpose of the review was to evaluate TPHC's compliance with HIPAA and the HITECH regulations, including best practices and relevant County and Departmental policies and procedures. The scope of this review included the *HIPAA Privacy Rule and HITECH Act Audit Tool*, which is a general assessment to determine whether the TPHC is compliant with privacy, security, training, policies and procedures, and breach notification requirements. We noted that DPH follows the Department of Health Services' (DHS) HIPAA policies and procedures until they implement their own.

Our review covered the Privacy Rule requirements for: 1) notice of privacy practices (NPP) for protected health information (PHI), 2) safeguards for PHI, 3) training, 4) complaint process, 5) refraining from intimidating or retaliatory acts, 6) uses and disclosures requiring authorization, 7) accounting for disclosures of PHI, 8) minimum necessary rule, and 9) HITECH Act Breach Notification Rule.

¹ 45 Code of Federal Regulations (CFR) Parts 160 and 164

Results of Review and Recommendations

Notice of Privacy Practices (NPP)

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.²

TPHC management reported that all patients are given the NPP on their first service delivery date. We reviewed five randomly selected patient charts, and noted they all included the required acknowledgement of receipt.

During our facility walk-through, we found that while the NPP was prominently posted in the patient waiting room, it did not include current contact information for U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), the County's Chief HIPAA Privacy Officer (CHPO), and DPH's Privacy Officer, as required.

TPHC is in partial compliance with the NPP standards.

Recommendation

- 1. Torrance Public Health Center management post updated Notice of Privacy Practices with current contact information for the three agencies listed above.**

DPH's response indicates that they implemented our recommendations and are compliant with the Notices of Privacy Practices' posting standards.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI, and prevent any disclosures that violate the Privacy Rule.

TPHC management reported that their computers are protected by endpoint protection software, which blocks downloading of PHI or other data to portable storage devices. In addition, TPHC computers are configured to prevent workforce members from saving PHI onto their hard drives. We verified that the fax machine, copier, and network printer were maintained in secure area, and no PHI was left unattended on or near these office equipment during our review.

² Ibid., §164.520(c)

TPHC management stated that medical charts are stored in the business office, which is kept locked at all times, and only employees who have a business need can access the office. During our site visit, we confirmed that the medical records are kept in a storage room inside the business office which was locked. We also noted that a security guard sits outside of the office, providing an added safeguard for the PHI.

While medical records appear to be secured, we noted that the facility did not adequately safeguard patients' x-ray films. Specifically, x-ray films were placed in jackets, labeled with patients' medical records numbers, and left on open shelves in the Radiology room, which was unlocked. We also noted that the Radiology room is sometimes left unattended when the technician/nurse leaves, and TPHC management does not restrict access to that area. This could allow PHI stored in the Radiology room to be compromised. TPHC management stated that they plan to purge all x-ray films by June 2014.

It appears that TPHC is in partial compliance with the Safeguards for PHI standards.

Recommendation

- 2. Torrance Public Health Center management ensure that x-ray films are properly secured, and restrict access to areas where protected health information is stored to employees who have a business need.**

TPHC management indicates that they have removed the x-ray films from the open shelves in the Radiology room, and Radiology staff has been instructed to keep the x-ray room secured and locked in their absence.

Training

TPHC, as a HIPAA covered program, must train all members of its workforce on policies and procedures related to PHI as required by the HIPAA Privacy and Security Rules, to the extent necessary and appropriate for them to do their jobs. Workforce members include employees, volunteers, and trainees.

The DPH Office of Organizational Development and Training is responsible for ensuring its workforce members are trained on HIPAA compliance via the Learning Net. TPHC management trains workforce members on DPH's HIPAA policies and procedures and additional, role-based training for their workforce members when applicable.

Our review of TPHC training records showed that all workforce members have completed the required HIPAA training. TPHC management confirmed that they also trained workforce members on the DHS HIPAA policies, which are placed in a binder and accessible via the Department's intranet site. It appears that TPHC is in compliance with the HIPAA training standards.

Complaint Process

A covered entity must provide a process for patients to complain about its policies and procedures. In addition, a covered entity must document all complaints received and their disposition, if any.

TPHC management informed us that the patient complaints are handled in accordance with DHS Policy 361.11, *Complaints Related To the Privacy of Protected Health Information (PHI)*, and the facility's own procedure and complaint form, and employees are trained to direct patients to contact the TPHC Privacy Coordinator to file a complaint. We reviewed the documents provided by TPHC management and noted that the facility has the required HIPAA complaint process in place.

In the past year, no HIPAA complaints were filed with the CHPO by TPHC patients. It appears that TPHC is in compliance with complaint standards.

Refraining from Intimidating or Retaliatory Acts

Discussions with TPHC management confirm they are aware of their obligation to comply with DHS Policy 361.13, *Non-Retaliation*. They also understand that OCR will investigate complaints against a covered entity that assert retaliatory actions. In the past year, no complaints related to retaliatory or intimidating acts were filed with the CHPO by TPHC patients. It appears that TPHC is in compliance with the non-retaliation standards.

Uses and Disclosures Requiring Authorization

OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including: (1) a description of the PHI to be used and disclosed, (2) the person authorized to make the use or disclosure, (3) the person to whom the covered entity may make the disclosure, (4) an expiration date, and (5) the purpose for which the information may be used or disclosed.

TPHC management reported that they follow DHS Policy 361.4, *Use And Disclosure of Protected Health Information (PHI) Requiring Authorization*, until DPH implements its own, and DPH Form H196, *Authorization For Uses And Disclosures of Protected Health Information*. We reviewed both documents and determined that they meet the Uses and Disclosures Requiring Authorization standards. While the charts that were randomly selected as part of our review did not include copies of authorizations as they were not required, discussions with TPHC management indicate that workforce members are trained on the uses and disclosures to PHI standards and adhere to them.

Accounting for Disclosures of Protected Health Information

The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, for up to six years after the disclosure. The following disclosures of PHI are excluded from the accounting requirement: (1) to the patient, (2) for treatment, (3) for payment and health care operations, (4) for facility directories, (5) pursuant to authorization, (6) pursuant to a limited data set agreement, (7) to persons involved in the patient's care, (8) for correctional institutions, and (9) for certain law enforcement purposes. In addition, an accounting of disclosures' log must be maintained in each patient's medical chart.

TPHC management reported that they follow DHS Policy 361.21, *Accounting of Disclosures of Protected Health Information* to track all non-routine disclosures. However, to date they have not received any patient requests for an accounting of disclosures. We provided additional guidance regarding accounting of disclosures to TPHC management following the review. TPHC appears to be in compliance with the Accounting for Disclosures of PHI standards.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, the Privacy Rule requires a covered entity to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is necessary for a particular purpose.

Discussions with TPHC management indicate that workforce members are aware of the minimum necessary standards. It appears that TPHC is in compliance with the Minimum Necessary Rule standards.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers to notify patients when their health information is breached. Specifically, health care providers and other covered entities must promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary annually. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate. Further, HHS' Breach Notification regulations emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured PHI.

TPHC management informed us that while they have not experienced a breach in their program, the workforce members are aware that they must report all incidents involving suspected or actual breaches to their immediate supervisors, who will report to DPH Privacy Officer. We noted from our review that DPH has a draft policy, *Responding to Breach or Suspected Breach of Protected Health Information*, and that it provides clear guidelines to workforce members in the event a breach or suspected breach of PHI is discovered. However, as of the date of this report, the final policy had not been issued to staff.

Recommendation

3. Department of Public Health management finalize its breach notification policy, and train workforce members on it.

DPH's response indicates that they are in the process of finalizing their breach notification policy for implementation.

Conclusion

Overall, our review indicates that TPHC management is aware of and has made substantial efforts to comply with the HIPAA Privacy regulations. However, DPH's Office of Administrative Deputy needs to work and assist TPHC to address the deficiencies noted in our review, and report any corrective action taken or pending to the HIPAA Compliance Office within 120 days from the receipt of this report. We also wish to thank DPH's Privacy Officer and TPHC managers and staff for their cooperation and assistance during this review.

Please call me if you have any questions, or your staff may contact Julia Chen, Assistant HIPAA Privacy Officer, at (213) 974-8315.

WLW:RGC:GZ:LTM:JC

Attachment

c: William T Fujioka, Chief Executive Officer
John F. Krattli, County Counsel
Robert Pittman, Chief Information Security Officer, Chief Information Office
David Dykstra, Administrative Deputy, Department of Public Health
Judy Tan, Privacy Officer, Department of Public Health
Audit Committee
Health Deputies

COUNTY OF LOS ANGELES • DEPARTMENT OF PUBLIC HEALTH
COMMUNITY HEALTH SERVICES

December 10, 2013

TO: Judy Tan
DPH Compliance Officer

FROM: Deborah Davenport, RN, MSPA
Director, CHS



SUBJECT: **HIPAA AND HITECH ACT COMPLIANCE REVIEW
TORRANCE PUBLIC HEALTH CENTER**

This memo is in response to the Auditor's draft report on the audit review of the Torrance Public Health Center (TPHC) that was conducted on September 9, 2013. Please note this response does not include Recommendation #3 which is a departmental level issue and action, and we believe requires your direct response as DPH Compliance Officer.

Recommendation #1:

Torrance Public Health Center management post updated Notice of Privacy Practices with current contact information for the three agencies listed above.

Response:

Agree: The Notice of Privacy Practices (NPP) have been updated and posted with current contact information for U.S. Department of Health and Human Services Office of Civil Rights, the County's Chief HIPAA Privacy Officer, and DPH's Privacy Officer. Please note that at the time of the audit, CHS had not yet been notified of the updated NPP contact information. This same notice was posted at Hollywood-Wilshire Health Center during a HIPAA audit approximately 6 months prior to the audit at Torrance, but no note of the information being incorrect was made at that time.

Recommendation #2:

Torrance Public Health Center management ensures that x-ray films are properly secured, and restrict access to areas where protected health information is stored to employees who have a business need.

December 10, 2013

Page 2

Response:

Agree: TPHC Radiology staff have removed x-ray film from the open shelves in the Radiology room, and secured the room. TPHC Radiology staff has been instructed to keep the x-ray area secured and locked in their absence.

Thank you for your assistance on this issue. My secretary Patricia Negrete can assist in scheduling the exit conference. If you have questions or need additional information, please let me know.

c: David Dijkstra, OAD
Robert Gibson
Patricio di Donato